Analyzing the effectiveness of the quantum repeater

Kenichiro Furuta, Hirofumi Muratani, Taichi Isogai and Tomoko Yonemura

Corporate Research & Development Center, Toshiba Corporation,
1, Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582, JAPAN
E-mail: {furuta,muratani,isogai,yonemura}@isl.rdc.toshiba.co.jp

Abstracts The communication distance of QKD is limited by exponential attenuation of photons propagating through optical fibers. However, it has been shown that introducing a quantum repeater can improve the order of the attenuation and is useful for extending the communication distance of QKD when the repeater noise is ignored. In this paper, we analyze the effectiveness of the quantum repeater when taking the repeater noise into consideration. We analyze the effectiveness also from the viewpoint of the security and show that QKD is secure even if a quantum repeater is used.

1 Introduction

There is an everlasting threat that a current practical cryptographic scheme whose security is based on computational assumptions will become insecure due to a future improvement of computers. Therefore, *quantum key distribution* (QKD), e.g. BB84[2] and B92, has been attracting considerable attention because its security is based only on quantum principles and it is unconditionally secure.

Due to exponential attenuation of photons in the channel, the naive QKD is valid only in the range of short distance. It is important to extend the communication distance from a practical viewpoint. So far, three approaches have been proposed to extend the range of QKD:

1.Protocol modification for multiple photon emission: Protocol modifications[7] which make the scheme robust against the photon number splitting(PNS) attack were proposed. However, modified protocols can extend the range of QKD to only a few times that of the original. Due to this limit, further extensions require introduction of other improvements.

2.Coherent states: Some protocol using coherent states[1] were proposed. It was demonstrated that they are more resistant to noises than the single photon protocols and can achieve high bit rate even in long distance. However, its security has been discussed enthusiastically[6, 8]. In this paper, we do not consider this.

3.Quantum repeater protocol: In order to reduce noises on quantum state transferred through the optical fiber, quantum teleportation is used to send the quantum state by using an EPR pair generated by a quantum repeater protocol. We call such a scheme *QKD with quantum repeater*. The quantum repeater recursively applies *entanglement swapping*(ES) and *entanglement purification protocol*(EPP) to short-length-EPR pairs[4]. It was demonstrated in [4] that

a quantum repeater protocol can generate the long-length-EPR pair for the quantum teleportation with high fidelity.

At a glance, the quantum repeater seems to be the most promising approach of the three approaches. However, the discussion in [4] seems to assume that noises in quantum memory on checkpoints can be negligible. Therefore, we reexamine the practical possibility of the quantum repeater by evaluating the order of the bit rate with considering the repeater noise. Although the repeater noise is noticed in [5], the evaluation is done without the repeater noise. We also examine the security of QKD with quantum repeater.

In Section 2, we review the quantum repeater protocol in [4]. In section 3, we categorize noises that occur in the protocol. In Section 4, we evaluate the bit rate without considering the repeater noise. In Section 5, we evaluate the bit rate with considering the repeater noise. In Section 6, we prove the security of QKD with quantum repeater. In Section 7, we provide a summary of this paper.

2 Quantum repeater protocol

The quantum repeater is a scheme which extends the length of an EPR pair with high fidelity. In this section, we review the quantum repeater protocol in [4].

2.1 Abstract specification

We explain an abstract specification of the quantum repeater protocol. The protocol recursively applies ES and EPP to short-length-EPR pairs and finally generates a long-length-EPR pair with high fidelity.

Let L be the number of EPR pairs which are linked in a single ES execution, N be the number of checkpoints and n be the depth of the recursive executions. These satisfy a relation, $N = L^n$. In the channel between the sender A and the receiver B, $N-1$ checkpoints, denoted $C_1, C_2, \cdots, C_{N-1}$, are settled. For convenience, A and B are denoted C_0 and C_N, respectively. The distance between A and B is denoted as D and the distance between two adjacent checkpoints is denoted as d. That is, $D = Nd$.

Then, quantum repeater protocol can be written as follows.

- Initialization: At each checkpoint C_i, $i = 0, \cdots, N-1$, EPR pairs are generated and one photon of each pair is sent to the next checkpoint C_{i+1}.
- FOR$x = 1$ to n
  - ES: Execute ES in each of the checkpoints $C_{kL^{x-1}}$,$(k = 1, 2, \cdots, N/L^{x-1})$ except C_{L^x}, C_{2L^x}, $\cdots, C_{N-L^x}$. Then, the EPR pairs of length L^x can be obtained.
  - EPP: Execute EPP for EPR pairs in each of the checkpoints $C_{L^x}, C_{2L^x}, \cdots, C_{N-L^x}$.

- Then, the EPR pairs of length L^x with high fidelity can be obtained.

After completing the above protocol, an EPR pair with high fidelity shared between C_0 and C_N is obtained.

2.2 Entanglement swapping

In ES, partners of two EPR pairs are swapped. Here, we provide an explicit realizations of ES based on local measurement. ES can also be realized based on Bell measurement.

First, Controlled NOT gate (CNOT) is applied to photons 2 and 3 of $|\phi^+\rangle_{1,2}\otimes |\phi^+\rangle_{3,4}$. Next, WH(Walsh-Hadamard) transformation is applied and produces $\frac{1}{2}(|0\rangle_2|0\rangle_3\otimes|\phi^+\rangle_{1,4}+|0\rangle_2|1\rangle_3\otimes|\psi^+\rangle_{1,4}+|1\rangle_2|0\rangle_3\otimes|\phi^-\rangle_{1,4}+|1\rangle_2|1\rangle_3\otimes|\psi^-\rangle_{1,4})$. Then, one of four computational bases of photons 2 and 3 is measured and this measurement maps the state of two photons 1 and 4 into a Bell state. Here, the observed basis of photons 2 and 3 indexes the projected Bell state of photons 1 and 4. In the next step, the projected Bell state of photons 1 and 4 is transformed into $|\phi^+\rangle$. For this purpose, the measurement results of photons 2 and 3 are sent from a checkpoint having photons 2 and 3 to ckechpoints having photons 1 and 4 with the classical communication.

2.3 Entanglement purification

EPP pulls out an EPR pair of high fidelity from multiple EPR pairs of low fidelity. We consider an EPP which is also considered in [4].

The validity of EPP requires that the fidelity of EPR pairs before the purification should be in a certain range. It is demonstrated as follows. Let F and $F^{'}$ be the fidelity of the EPR pairs before EPP and the fidelity of purified EPR pair, respectively. In the case that EPP generates the purified pair from two EPR pairs, F' can be expressed in terms of F as follows[3]:

$$F' = \Phi/\Lambda,\ where \bar{F} = (1-F)/3, \Phi = F^2 + \bar{F}^2 and \Lambda = F^2 + 2F\bar{F} + 5\bar{F}^2. \quad (1)$$

In order that $F^{'} \geq F$ in Eq.(1), F should be in the range of $1/2 \leq F \leq 1$.

3 Noises

Here, we categorize possible noises which occur during an execution of the protocol.

3.1 Noises during the protocol execution

Several types of noises can occur during the execution of the quantum repeater protocol. We classify them by their causes. The measurement noise is noises which occur during a measurement of a quantum state. The one-qubit operation noise is noises which occur during a one-qubit operation in the protocol. The

two-qubit operation noise is noises which occur during a two-qubit operation in the protocol. The channel noise is noises of a quantum state transferring through the channel. The repeater noise is noises of a quantum state in the repeater devices even in the absence of operation. Here, the one-qubit operation and the two-qubit operation mean a unitary operation on one qubit and a unitary operation on two qubits, respectively. We consider that quantum noises which occur during the classical communication in the execution of EPP or quantum teleportation is an example of the repeater noise.

The first three noises were modeled and analyzed in [4]. For the channel noise and the repeater noise, we evaluate with the order, such as exponential or polynomial. We review the models and analyses of the first three noises in the next subsection.

3.2 Conventional models and analysis

We show models of such noises and the modification of Eq.(1) caused by these noises. Let ρ be a density matrix before operations. First, the one-qubit operation noise is modeled as $\rho \rightarrow O_1\rho = p_1 O_1^{ideal}\rho + \frac{1-p_1}{2} tr_1\rho \otimes I_1$, where O_1 and O_1^{ideal} are one-qubit operations with and without the noise, respectively, and I_1 is the identity operator and p_1 is the probability with which the operations are performed without noise. The two-qubit operation noise is modeled as $\rho \rightarrow O_{12}\rho = p_2 O_{12}^{ideal}\rho + \frac{1-p_2}{4} tr_{12}\rho \otimes I_{12}$, where O_{12} and O_{12}^{ideal} are two-qubit operations with and without the noise, respectively, and I_{12} is the identity operator and p_2 is the probability with which the operations are performed without noise. The measurement noise is modeled as $P_0^\eta = \eta|0\rangle\langle 0| + (1-\eta)|1\rangle\langle 1|, P_1^\eta = \eta|1\rangle\langle 1| + (1-\eta)|0\rangle\langle 0|$, where η is the probability with which the measurements are performed correctly and P_0^η and P_1^η are POVM $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, respectively, with error probability η.

Based on the above noise models, the fidelity, F_L, after linking L EPR pairs by ES executions is expressed as $F_L = \frac{1}{4} + \frac{3}{4}\left(\frac{p_1^2 p_2(4\eta^2-1)}{3}\right)^{L-1}\left(\frac{4F-1}{3}\right)^L$. Similarly, based on the above noise models, the change of the fidelity by EPP is expressed as follows:

$$F' = \{\Theta\Phi + 2\eta\bar{\eta}\Xi + \Pi\}/\{\Theta\Lambda + 4(2\eta\bar{\eta}\Xi + \Pi)\}, \tag{2}$$

where $\bar{\eta} = 1-\eta$, $\Theta = \eta^2 + \bar{\eta}^2$, $\Xi = F\bar{F} + \bar{F}^2$ and $\Pi = \frac{1-p_2^2}{8p_2^2}$. F and $F^{'}$ have three intersections. Let two intersections except 0.25 be $F_{min} and F_{max}$, where $F_{min} < F_{max}$. Then, in order that $F^{'} \geq F$ in Eq.(2), F should be in the range of $F_{min} \leq F \leq F_{max}$. The range of F where the quantum repeater is valid become narrow as noises become large.

4 Bit rate in absence of repeater noise

In [4], it was demonstrated that the required amount of resources of the quantum repeater increases as a polynomial function of the distance between A and B, D.

This leads to the conclusion that the bit rate of the quantum repeater decreases as an inverse of a polynomial function of the distance. This result was derived under the condition that only the channel noise, the measurement noise, the one-qubit operation noise and the two-qubit operation noise are considered.

Theorem 1. *Consider QKD with quantum repeater. If only the channel noise, the measurement noise, the one-qubit operation noise and the two-qubit operation noise are considered, there exists a polynomial function $p(\cdot)$ such that the bit rate of the QKD decreases as $\Omega(p(D)^{-1})$.*

Here, $g(n) = \Omega(f(n))$ means $\exists c > 0\, \exists N \in \mathbb{N}\, \forall n > N\, g(n) \geq cf(n)$.

proof. The bit rate is estimated by considering both the merit of quantum repeater, keeping high fidelity, and the demerit, increase of resource.

Let M be the number of EPR pairs consumed by a single execution of EPP. Then, the number of EPR pairs, R, in the whole execution of the quantum repeater, is $R = (LM)^n = L^n M^n = NM^n = N(L^{\log_L M})^n = N^{\log_L M+1}$, where N is proportional to the communication distance D, and L and M do not depend on D. Thus, R is a polynomial function of D.

In this scheme, when not considering the repeater noise, the fidelity of the EPR pair generated by the quantum repeater protocol stays constant even if D increases. So, the bit rate of the QKD decreases as $\Omega(p(D)^{-1})$. □

In contrast to exponential damping in the absence of the quantum repeater, the bit rate of QKD in the presence of the quantum repeater decreases as an inverse of a polynomial function of the communication distance. Although Theorem 1 does not indicate whether the exact value of the bit rate is really improved by the quantum repeater, it can be expected to be effective for sufficiently large D.

5 Bit rate in presence of repeater noise

We next consider the case the repeater noise is taken into account. In ES and EPP in the quantum repeater protocol, classical communications between repeater devices are needed. In addition, quantum teleportation sends classical information from A to B. During these classical communications, the quantum states in the repeater devices lose their fidelity. We assume the repeater noise as follows: The fidelity of a quantum state in a repeater device decreases exponentially with respect to the time length of a classical communication. We call the assumption of this model *the exponential damping assumption.*

Theorem 2. *Under the exponential damping assumption, the bit rate of QKD with quantum repeater decreases asymptotically exponentially with respect to the distance D.*

proof. The length of EPR pairs increases as the quantum repeater protocol proceeds. As far as the length is small, the fidelity can be recovered by EPP.

However, if the length exceeds a threshold, D_{th}, then the fidelity becomes lower than F_{min} and EPP can't recover the fidelity any more. The reason is that EPR pairs have to stay in quantum memory on ckeckpoints during classical communication and the time of classical communication becomes large as the length of EPR pairs become large. Thus, time of being affected by the repeater noise get larger. After the fidelity goes under the threshold of EPP, the fidelity continues to decrease as the quantum repeater protocol proceeds. So, after crossing the threshold, $\Delta F_{ES} + \Delta F_{EPP} + \Delta F_{RN} \geq \Delta F_{RN}$, where $\Delta F_{ES}, \Delta F_{EPP}$ and ΔF_{RN} are the fidelity decreases due to ES, EPP and the repeater noise, respectively, during an iteration in the recursive execution of the quantum repeater protocol. The dumping due to the repeater noise is exponential according to the exponential dumping assumption. So, the overall dumping is exponential according to the equation above. □

Of course, there may be many other quantum repeater protocols. However, in general, our result holds for protocols as long as the classical communication whose distance is proportional to the distance between a sender and a receiver is used in the protocols.

So, it is important to suppress the repeater noise as small as possible. As the repeater noise gets smaller, the range where quantum repeater can improve the bit rate becomes wide.

6 Security

The security proof can be done with simple idea. Let I_E be the amount of eavesdropper's information and P_{cont} be the person who controls the quantum repeater unit and Eve be an eavesdropper. The following relationship holds for I_E. (I_E in original QKD)$\geq$ (I_E in QKD with quantum repeater, where P_{cont} is Eve)$\geq$ (I_E in QKD with quantum repeater, where P_{cont} is except Eve).

The reason is as follows. For QKD with quantum repeater, Eve can get more information (or equal at least) when he controls repeater unit more than when he does not. So, (I_E in QKD with quantum repeater, where P_{cont} is Eve)$\geq$ (I_E in QKD with quantum repeater, where P_{cont} is except Eve). Thus, it is sufficient to prove the security when repeater unit is controlled by Eve. Here we deal with QKD protocols where operations for quantum repeater protocol can be done within attacks allowed for Eve in original QKD protocol. Unconditionally secure protocols, such as BB84[2], belong to this category because Eve is allowed to do almost every quantum operations as attacks. So, when repeater unit is controlled by Eve, operations for quantum repeater can be considered as a part of Eve's attacks allowed in original QKD. Then, (I_E in original QKD)$\geq$ (I_E in QKD with quantum repeater, where P_{cont} is Eve). Thus, we can turn the proof of QKD with quantum repeater into the proof of original QKD.

7 Summary

We demonstrated that the bit rate of QKD with quantum repeater decreases asymptotically exponentially with respect to the communication distance when the repeater noise is taken into account. This is because EPP can not work when the length of EPR pairs exceed the threshold. In contrast, quantum repeater protocol works when the length of EPR pairs does not exceed the threshold. This threshold depends on the largeness of the repeater noise. So, it is important to suppress the repeater noise in order to enlarge the range where quantum repeater is effective. Besides, we showed abstract of proof that QKD with quantum repeater is secure.

References

[1] G. Barbosa, E. Corndorf, P.Kumar, and H. Yuen. Secure Communication Using Mesoscopic Coherenet States. *Phys. Rev. Lett.*, Vol. 90, p. 227901, 2003.

[2] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE New York)*, pp. 175–179, 1984.

[3] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.*, Vol. 76, No. 5, pp. 722–725, 1996.

[4] H.J. Briegel, W. Dür, J.I. Cirac, and P. Zoller. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.*, Vol. 81, No. 26, pp. 5932–5935, 1998.

[5] L. Childress, J.M. Taylor, A.S. Sørensen, and M.D. Lukin. Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single photon emitters. *quant-ph/0502112*, 2005.

[6] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai. How much security does Y-00 protocol provide us? *Phys. Lett. A*, Vol. 327, pp. 28–32, 2004.

[7] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.*, Vol. 92, No. 5, p. 057901, 2004.

[8] H. Yuen, E. Corndorf, G. Barbosa, and P. Kumar. Barbosa et al. Reply:. *Phys. Rev. Lett.*, Vol. 94, No. 4, p. 048902, 2005.